Quantum coding theorem from privacy and distinguishability

Michał Horodecki
Institute of Theoretical Physics and Astrophysics, University of Gdánsk, Poland

Seth Lloyd
Massachusetts Institute of Technology, Cambridge, MA 02139 USA

Andreas Winter
Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, U. K.

We prove direct quantum coding theorem for random quantum codes. The problem is separated into two parts: proof of distinguishability of codewords by receiver, and of indistinguishability of codewords by environment (privacy). For a large class of codes, only privacy has to be checked.

arXiv:quant-ph/0702006v1 31 Jan 2007

I. INTRODUCTION

The quantum coding theorem for transmission of quantum information via noisy channel is one of the fundamental achievement of quantum information. First proof for direct codign theorem was given in [1]. Though not fully rigorous, it contains all essntial ingredients. We hope that soon complete version of the proofs will appear. The converse theorem was rigorously proven in [2] (see [3] in this context). An attmept to rigourous proof of direct coding theorem was done by Shor, with his notes published on website [4]. Later, Devetak provided first complete proof of coding theorem, using so called random CSS codes. Both for practical as well as for fundamental reasons it is desirable to have proof of coding theorem for fully random codes, such as Lloyd, or Shor ones. In this paper we present a new proof of coding theorem. The main advantage of the present approach, is that we divide problem of coding theorem into two separate problems. One is whether Bob can distinguish signals, the second is whether environmenet cannot distinguish them. It is well known that those two conditions are crucial for sending quantum information reliably. The first one is connected with bit error, and the second with phase error [1, 4, 5, 6]. Actually, Devetak's coding scheme is a coherent version of cryptographic protocol consisting of two stages: error correction, that ensures distinguishability by Bob and privacy amplification responsible for diminishing Eve's knowledge.

However so far the two problems have not been separated, in the sense, that the proof of coding theorem did not consisted of two completely separate mathematical problems.

More specifically, we show that if we have set of N vectors which, after crossing the channel are distinguishable for Bob (receiver), but not for Eve (controlling environment), then Alice (sender) and Bob can share maximally entangled state of rank N. The statement of quantum coding theroem, is that capacity is determined by coherent information I_{coh} [7]. Thus the question whether for n uses of the channel, the set of vectors (quantum code) that satisfy the two conditions can have $2^{nI_{coh}}$ elements.

In classical case the coding theorem states that capacity is determined by Shannon mutual information I_M. Since only distinguihability is needed, one proceeds as follows. One fixes source, and then pick codewords at random from the probability distribution of the source. Such a randomly chosen code can have size as large as 2^{nI_M} and still be distinguishable after passing the channel.

In quantum case two problems arise. Firstly, as we have mentioned, we need two things: not only distinguishability by Bob, but also indistinguishability by Eve (one can call it "privacy"). Secondly, for a fixed source, unlike in classical case, we have many different ensembles which are compatible with the source. Thus "picking random code" is not uniquely defined, so that we have to choose an ensemble. The advantage of our approach, is that we will see that various ensembles can do the job. It turns out that arbitrary ensemble, if we pick at random $2^{nI_{coh}}$ vectors, they will be distinguishable for Bob. This we obtain adapting a lemma proven by Devetak [8] - a one-shot version of HSW theorem.

Thus to know that a given code is good, we need only to check privacy. It is easy to see that this will no longer hold for arbitrary ensebmle. To assure privacy, the ensemble must be reach enough. It turns out that checking privacy for some ensembles is a fairly easy task. In this paper we will do this for ensemble used by Lloyd, and for ensemble generated by Haar measure, deformed by source. Most likely, it also works for Gaussian codes (also deformed by source).

II. QUANTUM ERROR - ANALOGUE OF CLASSICAL ERROR PROBABILITY

Here we will introduce a quantum parameter analogous to error probability in classical coding theorem. The main points have been already found in [9], in a slightly different form.

We need the following lemma, which says that when Alice is product with environment (Eve) then there exists Bob decoding, after which he shares with Alice pure state which is purification of Alice's system

Lemma 1 *For any pure tripartite state ψ_{ABE}, if reduced state ρ_{AE} is product, then there exists unitary operation $U_{BB'}$, such that*

$$I_{AE} \otimes U_{BB'}|\psi_{ABE}\rangle|0\rangle_{B'} = |\psi_{AB}\rangle|\psi_{EB'}\rangle \tag{1}$$

Proof. Follows from the fact that all purifications of a fixed state are related by a unitary transformation on (perhaps extended) ancilla. Here we take the state to be σ_{AE} and extended ancilla system is BB' Without loss of generality we have assumed here that the system B is not smaller than A. ∎

Here is version of the above lemma in approximate case.

Lemma 2 *Consider a state ψ_{ABE} and suppose that*

$$||\sigma_{AE} - \sigma_A \otimes \sigma_E||_{\mathrm{Tr}} \leq \epsilon \tag{2}$$

Then there exists unitary $U_{BB'}$ such that

$$F(\sigma'_{AB}, \phi_{AB}) \geq 1 - \frac{1}{2}\epsilon \tag{3}$$

where σ'_{AB} is reduced density matrix of state $I_{AE} \otimes U_{BB'}|\psi_{AEB}\rangle|0\rangle_{B'}$ and ϕ_{AB} is purification of σ_A (reduced density matrix of ψ_{ABE}).

Proof. Using inequality $F(\rho,\sigma) \geq 1 - \frac{1}{2}||\rho - \sigma||$ [10] we get $F(\sigma_{AE}, \sigma_A \otimes \sigma_B) \geq 1 - \epsilon/2$. Then, by definition of F, there exists purification $\phi_{ABB'E}$ such that

$$F(|\psi_{ABE}\rangle|0\rangle_{B'}, \phi_{ABB',E}) = F(\sigma_{AE}, \sigma_A \otimes \sigma_B) \geq 1 - \frac{1}{2}\epsilon \tag{4}$$

From the proof of previous lemma, we see that there exists unitary operation $U_{BB'}$ which factorizes state ϕ into B and B' (again we assume here that dimension of the system B is no smaller than that of A). Thus

$$F(\psi'_{ABB'E}, \phi'_{AB} \otimes \phi'_{EB'}) \geq 1 - \frac{1}{2}\epsilon \tag{5}$$

where $|\psi'_{ABB'E}\rangle = I_{AE} \otimes U_{BB'}|\psi_{ABE}\rangle \otimes |0\rangle$ and $\phi'_{AB} \otimes \phi'_{EB'} = I_{AE} \otimes U_{BB'}|\phi_{ABB'E}\rangle$. Note that ϕ'_{AB} is purification of σ_A From monotonicity of F under partial trace we get:

$$F(\sigma'_{AB}, \phi_{AB}) \geq 1 - \frac{1}{2}\epsilon \tag{6}$$

This ends the proof of the lemma. ∎

It says that if Alice and Eve are approximately product, then there exists Bob's decoding, which restores with high fidelity of entanglement with Alice.

Thus the parameter $||\sigma_{AE} - \sigma_A \otimes \sigma_E||_{\mathrm{Tr}}$ is what we could call "quantum error", an analogue of error probability in classical coding theorems.

It is however convenient to consider modified quantum error, which, if small, implies that Alice and Bob share a state close to maximally entangled state of Schmidt rank N. Henceforth in paper we will us this type of quantum error. It is given by

$$q_e = \|\sigma_{AE} - \tau_A \otimes \sigma_E\| \tag{7}$$

where τ is normalized projector of rank N. From the above lemma we obtain the main result of this section:

Proposition 1 *Consider arbitrary pure state ψ_{ABE}. Let σ_{AB} be reduced density matrix of ψ_{ABE}. Then, for arbitrary $\epsilon > 0$ if the quantum error (7) satisfies*

$$q_e \leq \epsilon \tag{8}$$

then there exists Bob's operation Λ_B such that

$$F(\sigma'_{AB}, \psi^+_{AB}) \geq 1 - \frac{1}{2}\epsilon \tag{9}$$

where $\sigma'_{AB} = (I_A \otimes \Lambda_B)\sigma_{AB}$, and $\psi^+_{AB} = \frac{1}{\sqrt{N}} \sum_{i=1}^N |ii\rangle$.

Therefore, the task is to find a bipartite state for Alice, such that if she will send half of it down the channel, then the quantum error will be small, for $N \simeq 2^{I_{coh}}$. We will construct such a state from a code. Given a code $\{|\alpha\rangle\}_{\alpha=1}^N$ the state will be

$$\psi_{AA'} = \frac{1}{\sqrt{N}} \sum_{\alpha=1}^N |\psi_\alpha\rangle|\alpha\rangle \tag{10}$$

The task is thus to show that, if A' is sent down the channel, then q_e is small.

III. DISTINGUISHABILITY AND PRIVACY IMPLY SMALL QUANTUM ERROR

The channel from Alice to Bob implies dual channel to Eve, who represents environment. Thus if Alice sends a state $|\alpha\rangle$, we obtain two kinds of output states: Bob's output state σ_B^α and Eve's output state σ_E^α. In this section we will show that a set of states $\mathcal{C} = \{|\alpha\rangle\}$ for which Bob's output states are approximately distinguishable, while Eve's output states are not, then the set $\mathcal{C}$ is a good quantum code. This means that if Alice will create state

$$\psi_{AA'} = \frac{1}{\sqrt{N}} \sum_{\alpha=1}^N |\psi_\alpha\rangle|\alpha\rangle \tag{11}$$

where ψ_α are orthonormal vectors. and send the system A' down the channel, then the quantum error for arising tripartite state ψ_{ABE} will be approximately zero. The distinguishability we will quantify by Holevo function.

Before we formulate suitable proposition, let us express output states of Bob and Eve in terms of the joint state ψ_{ABE} obtained as described above. If we perform measurement onto basis ψ_α, the state of the systems BE will collapse to the state ψ_{BE}^α. The states σ_B^α and σ_E^α are then given by

$$\sigma_B^\alpha = \mathrm{Tr}_E(|\psi_\alpha\rangle\langle\psi_\alpha|_{BE}), \quad \sigma_E^\alpha = \mathrm{Tr}_B(|\psi_\alpha\rangle\langle\psi_\alpha|_{BE}) \tag{12}$$

Let us now define more precisely distinguishability and privacy. For a set of N states $\mathcal{C} = \{\alpha\rangle\}$ and channel Λ let us define distinguishability by Eve $\mathcal{D}_E$ and distinguishability $\mathcal{D}_B$ as follows

$$\mathcal{D}_E = \chi_E \tag{13}$$
$$\mathcal{D}_B = \chi_B \tag{14}$$

where $\sigma_{E,B}^\alpha$ are Eve's and Bob's output states defined above and $\chi_E = \chi(\{\frac{1}{N}, \sigma_E^\alpha\}), \chi_B = \chi(\{\frac{1}{N}, \sigma_B^\alpha\})$.

Proposition 2 *The quantum error satisfies the following inequality*

$$Q_e \leq c\sqrt{\mathcal{D}_E + (\log N - \mathcal{D}_B)} \tag{15}$$

where $c = \sqrt{2\ln 2}$.

Proof. Let subsystems of ψ_{ABE} are denoted by σ_X and their entropies by S_X with suitable subscript. Because σ_B^α and σ_E^α are reduced density matrices of the same state ψ_{BE}^α we have

$$S(\sigma_E^\alpha) = S(\sigma_B^\alpha) \tag{16}$$

Thus

$$\chi_B - \chi_E = S_B - S_E \tag{17}$$

so that we obtain

$$\mathcal{D}_B + (\log N - \mathcal{D}_E) = \log N + S_E - S_{AE} = S(\sigma_{AE}|\tau_A \otimes \sigma_E) \tag{18}$$

where we have used the fact that total state is pure so that $S_{AE} = S_B$, and $\tau_A = I/N$ is maximally mixed state on the system A. Now, using well known relation $S(\rho|\sigma) \geq \frac{1}{2\ln 2}\|\rho - \sigma\|^2$ [11] we obtain the required inequality. This ends the proof of the proposition.∎

Remark. Essentially, we have merged two facts. First, as obtaind in [9] that when I_{coh} is close to entropy of the source, then the error correction condition is approximately satisfied. Second, that $\chi_B - \chi_E = I_{coh}$ which was exploited in [5, 6].

IV. OVERVIEW

In spirit of Shannon we will consider mental construction: a source ρ_A, and a joint state ϕ_{ABE} which emerges from sending half of a purification of ρ_A down the channel (as before, E represents environment). We will also use the state ϕ projected onto typical subspaces. This will be denoted by ϕ'_{ABE}. The two states ϕ and ϕ' will be shown to be close to each other in trace norm.

A code will be picked at random from ensemble which gives rise to typical version of ρ_A. Depending on chosen ensemble of ρ_A^{typ}, we will have different types of codes. For any code $\{|\alpha\rangle\}$ we will consider a bipartite state of Alice of the form $\psi_{AA'} = \frac{1}{\sqrt{N}}\sum_{\alpha=1}^N |\psi_\alpha\rangle|\alpha\rangle$. This is the *actual* state that will be will be sent down the channel. The resulting joint state of Alice, Bob and Eve will be denoted by $\psi_{ABE}(\mathcal{C})$ (shortly ψ_{ABE}). Again a version of this state, projected onto typical subspaces will be denoted by ψ'_{ABE}. We will show that for certain codes (i.e. for certain ensembles) the states ψ and ψ' are close to each other in trace norm.

Since the states are close to each other, it is enough to consider privacy and distinguishability for the projected state. Interestingly, we will show that distinguishability is then merely a consequence of the fact that the ensemble from which we choose the code gives rise to typical version of ρ_A. This we obtain by adapting one-shot version of HSW thereom proven by Devetak [8]. Privacy should be checked case by case for different codes.

V. SOURCE, CHANNEL AND TYPICALITY

Let us fix a source $\rho_A^{\otimes n}$. Half of purification of the source is sent down the channel

$$\Lambda^{\otimes n}(\cdot) = \sum_k A_k(\cdot)A_k^\dagger \tag{19}$$

(it is not real sending but a mental construction, as in classical coding theorem). This creates pure state $\phi_{ABE}^{\otimes n}$ shared by Alice, Bob and environment. Explicitly we have

$$\phi_{ABE} = \sum_{i\in I}\sum_{k\in K}\sqrt{p_i}|i\rangle_A A_k|i\rangle_B|k\rangle_E \tag{20}$$

where $\rho_A^{\otimes n} = \sum_{i\in I} p_i|i\rangle\langle i|$, I is set of indices of complete eigenbasis of $\rho_A^{\otimes n}$, and K is set of indices of complete eigenbasis of $\rho_E^{\otimes n}$. Later we will consider typical subspaces, and this we will indicate by omitting I and K.

Subsystems of this state are $\rho_A^{\otimes n}$, $\rho_B^{\otimes n} = \Lambda^{\otimes n}(\rho_A^{\otimes n})$ and $\rho_E^{\otimes n}$. Projectors onto typical subspaces of these states are respectively: Π_A, Π_B and Π_E. The (unnormalized) typical versions of the states we denote by $\hat\rho_A^{typ} = \Pi_A\rho_A^{\otimes n}\Pi_A$, $\hat\rho_B^{typ} = \Pi_B\rho_B^{\otimes n}\Pi_B$, $\hat\rho_E^{typ} = \Pi_E\rho_E^{\otimes n}\Pi_E$. Explicitly we have

$$\hat\rho_A^{typ} = \sum_i p_i|i\rangle\langle i| \tag{21}$$

$$\hat\rho_B^{typ} = \Pi_B\sum_{k\in K} A_k\rho_A^{\otimes n}A_k^\dagger\Pi_B \tag{22}$$

$$\hat\rho_E^{typ} = \sum_{k,k'}\mathrm{Tr}(A_k\rho_A^{\otimes n}A_k'^\dagger)|k\rangle\langle k'| \tag{23}$$

In second equation we write $k \in K$ because the sum runs over all vectors $|k\rangle$, while in first and third equation the sum runs only over the set of indices corresponding to vectors from typical subspace. We have to explain why typical projector Π_E is given by $\sum_k |k\rangle\langle k|$. This follows form the fact that the Kraus operators can be chosen in such a way that the state $\rho_E^{\otimes n}$ is diagonal. We assume that our Kraus operators are such ones (so that the only diagonal terms of the last equation are in fact nonzero).

We have lemma [12, 13, 14]

Lemma 3 *(typical states) For arbitrary $0 < \epsilon < 1/2$, $\delta > 0$, for all n large enough we have that for $X = A$, $X = B$ and $X = E$:*

1. *The states $\hat{\rho}_X^{typ}$ are almost normalized i.e.*

$$\mathrm{Tr}\hat{\rho}_X^{typ} \geq 1 - \epsilon \tag{24}$$

2. *All eigenvalues λ of $\hat{\rho}_X^{typ}$ satisfy*

$$2^{-n(S_X+\delta)} \leq \lambda \leq 2^{-n(S_X-\delta)} \tag{25}$$

3. *The ranks of states $\hat{\rho}_X^{typ}$ satisfy*

$$\mathrm{rk}\,(\hat{\rho}_X^{typ}) \leq 2^{n(S_X+\delta)} \tag{26}$$

Remark. Both in this lemma, and in Prop. 3, ϵ can be exponential in n, i.e. the relations hold with

$$\epsilon = e^{-c\delta^2 n} \tag{27}$$

where c is a constant.

Let us now consider an unnormalized state

$$|\tilde{\phi}_{ABE}\rangle = \Pi_A \otimes \Pi_B \otimes \Pi_E |\phi_{ABE}\rangle \tag{28}$$

The state can be written

$$|\tilde{\phi}_{ABE}\rangle = \sum_{i,k} \sqrt{p_i}|i\rangle_A F_k|i\rangle_B|k\rangle_E \tag{29}$$

where $F_k = \Pi_B A_k$.

The reductions of this state are a bit different than typical states $\hat{\rho}_X^{typ}$. We will denote them by $\tilde{\rho}_A$, $\tilde{\rho}_B$ and $\tilde{\rho}_B$. We have

$$\tilde{\rho}_A = \sum_i p_i|i\rangle\langle i|\mathrm{Tr}(\sum_k F_k|i\rangle\langle i|F_k^\dagger) \tag{30}$$

$$\tilde{\rho}_B = \Pi_B \sum_k A_k\hat{\rho}_A^{typ} A_k^\dagger \Pi_B = \sum_k F_k\hat{\rho}_A^{typ} F_k^\dagger \tag{31}$$

$$\tilde{\rho}_E = \sum_{k,k'} \mathrm{Tr}(F_k\hat{\rho}_A^{typ} F_k^\dagger)|k\rangle\langle k'| \tag{32}$$

Finally, we consider *normalized* typical Alice's state ρ_A^{typ} given by

$$\rho_A^{typ} = \frac{1}{\mathrm{Tr}\hat{\rho}_A^{typ}}\hat{\rho}_A^{typ} \tag{33}$$

We then modify the above states $\tilde{\rho}_A$, $\tilde{\rho}_B$ and $\tilde{\rho}_E$ into still unnormalized states

$$\rho'_B = \frac{1}{\mathrm{Tr}\hat{\rho}_A^{typ}}\tilde{\rho}_B = \Pi_B \sum_k A_k\rho_A^{typ} A_k^\dagger \Pi_B = \sum_k F_k\hat{\rho}_A^{typ} F_k^\dagger$$

$$\rho'_E = \frac{1}{\mathrm{Tr}\hat{\rho}_A^{typ}}\tilde{\rho}_E = \sum_{k,k'} \mathrm{Tr}(F_k\rho_A^{typ} F_k^\dagger)|k\rangle\langle k'|$$

$$\rho'_A = \frac{1}{\mathrm{Tr}\hat{\rho}_A^{typ}} \sum_i p_i|i\rangle\langle i|\mathrm{Tr}(\sum_k F_k|i\rangle\langle i|F_k^\dagger) \tag{34}$$

A. Properties of states ρ'_X

The states that we will use most frequently in the proof are ρ'_X. We have the following proposition

Proposition 3 *For arbitrary $0 < \epsilon < 1/2$, $\delta > 0$, for all n large enough we have that for $X = A$, $X = B$ and $X = E$:*

1. *The states ρ'_X are almost normalized i.e.*

$$\mathrm{Tr}\rho'_X \geq 1 - \epsilon. \tag{35}$$

2. *The eigenvalues λ of ρ'_X satisfy*

$$\lambda \leq (1+\epsilon)2^{-n(S_X - \delta)} \tag{36}$$

3. *The ranks of states ρ'_X satisfy*

$$\mathrm{rk}\,(\rho'_X) \leq 2^{n(S_X+\delta)}. \tag{37}$$

4. *The following inequality holds*

$$\mathrm{Tr}\rho'^2_X \leq (1+\epsilon)2^{(-nS_X-\delta)}. \tag{38}$$

Proof. We first note that $\tilde{\rho}_X \leq \hat{\rho}_X^{typ}$, which holds, because $\tilde{\rho}_X$ can be obtained from $\hat{\rho}_X^{typ}$ by projecting onto second subsystem of bipartite state, whose reduction is $\tilde{\rho}_X$. Using lemma 3, eq. (24) we then obtain that for large n

$$\rho'_X \leq (1+\frac{\epsilon}{4})\hat{\rho}_X^{typ} \tag{39}$$

This via lemma 3 immediately gives eq. (35) and eq. (36) as well as (37). To prove (38) we note that $0 \leq X \leq Y$ implies $\mathrm{Tr}X^2 \leq \mathrm{Tr}Y^2$. ∎

There follow useful expressions [1]

$$\sum_{k,k'} \mathrm{Tr}(F_k\rho_A^{typ}\,F_{k'}^\dagger)\mathrm{Tr}(F_{k'}\rho_A^{typ}\,F_k^\dagger) = \mathrm{Tr}\rho'^2_E \tag{40}$$

$$\sum_{k,k'} \mathrm{Tr}(F_k\rho_A^{typ}\,F_k^\dagger F_{k'}\rho_A^{typ}\,F_{k'}^\dagger) = \mathrm{Tr}\rho'^2_B \tag{41}$$

One also defines matrix

$$\rho_{i/o} = \frac{1}{\mathrm{Tr}\hat{\rho}_A^{typ}} \sum_{i,k} p_i|i\rangle_A\langle i| \otimes F_k(|i\rangle_B\langle i|)F_k^\dagger \tag{42}$$

One finds that reduced density matrices of $\rho_{i/o}$ are ρ'_A and ρ'_B. One can find by direct checking that

$$\mathrm{Tr}\rho_{i/o}^2 \leq \min(\mathrm{Tr}\rho'^2_B, \mathrm{Tr}\rho'^2_A) \tag{43}$$

VI. RANDOM CODES

As we have mentioned, in quantum case there is no unique way of drawing codes at random. In this paper we will use two types of quantum random codes: Lloyd codes defined in [1] and uniform, ρ_A^{typ}-distorted codes (modification of codes used by Shor in [4]. For those codes we will show that the average quantum error is small, if we choose 2^{nR} codewords, with $R < I_{coh}$.

Lloyd codes: The codes of [1] are defined as follows. To have a code consisting of N vectors, Alice picks N vectors according the following distribution

$$|\alpha\rangle = \sum_i \sqrt{q_i}e^{i\phi_i}|i\rangle \tag{44}$$

where q_i and $|i\rangle$ are eigenvalues and eigenvectors of ρ_A^{typ}, i.e. $q_i = p_i/\mathrm{Tr}\hat{\rho}_A^{typ}$. The phases ϕ_i are drawn independently and uniformly from unit circle. Average over such α's we will denote by $\int(...)\mathrm{d}\alpha$. Note that the ensemble defining Lloyd codes give rise to typical version of ρ_A

$$\int |\alpha\rangle\langle\alpha|\mathrm{d}\alpha = \rho_A^{typ}. \tag{45}$$

Uniform ρ_A^{typ}-distorted codes. Alice picks N vectors according to the following distribution

$$|\alpha\rangle = \sqrt{d_A}\sqrt{\rho_A^{typ}}|\phi\rangle \tag{46}$$

where $|\phi\rangle$ is taken uniformly from typical subspace of system A (i.e. give by projection Π_A. The codewords are not of unit length but with high probability they are almost normalized. We prove it by Chebyshev inequality. Compute variance of $\langle\alpha|\alpha\rangle = d_A\langle\phi|\rho_A^{typ}|\phi\rangle$ obtaining

$$Var = \frac{d_A^2}{d_A^2+d_A}\mathrm{Tr}(\rho_A^{typ})^2 + \frac{d_A^2}{d_A^2+d_A}\mathrm{Tr}\rho_A^{typ} - 1 \le \mathrm{Tr}(\rho_A^{typ})^2 \le (1+\epsilon)2^{-n(S_A-\delta)} \tag{47}$$

which gives

$$Prob(\langle\alpha|\alpha\rangle \notin (1-\epsilon, 1+\epsilon)) \ge 1 - \frac{(1+\epsilon)}{\epsilon^2}2^{-n(S_A-\delta)} \tag{48}$$

The last inequality comes from lemma 3, and holds for all n large enough. If we take $N = 2^{nR}$ with $R < I_{coh}$, we get that for arbitrarily fixed ϵ the probability of failure goes exponentially down for all codewords. However we will not use so strong result. It will be enough to know that a randomly picked codeword with high probability has norm close to 1. Finally, note that, again we have

$$\int |\alpha\rangle\langle\alpha|\mathrm{d}\alpha = \rho_A^{typ}. \tag{49}$$

VII. JOINT STATE ψ_{ABE} FOR A FIXED CODE SENT DOWN THAT CHANNEL.

In this section we discuss properties of the actual state that can be obtained by use of codes. The main result of this section is that with high probability, the state ψ_{ABE} is close to its version projected onto typical subspcaces. We will separately discuss the case of normalized and unnormalized codes. For normalized codes, the result follows solely from the fact the ensemble of the code gives rise to ρ_A^{typ}. For unnormalized codes one has to check it case by case (we will check it here for uniform ρ_A^{typ}-distorted codes).

A. Normalized codes

Having fixed a code $\mathcal{C} = \{|\alpha\rangle\}_{\alpha=1}^N$, Alice creates state

$$\psi_{AA'} = \frac{1}{\sqrt{N}}\sum_{\alpha=1}^N |\psi_\alpha\rangle_A \otimes |\alpha\rangle_{A'} \tag{50}$$

where $\{|\psi_\alpha\rangle\}_{\alpha=1}^N$ is orthonormal set of N vectors. Then she sends A' down the channel $\Lambda^{\otimes n}$ to Bob. The emerging state ψ_{ABE} is the following:

$$\psi_{ABE} = \psi_{ABE}(\mathcal{C}) = \frac{1}{\sqrt{N}}\sum_\alpha\sum_{k\in K}|\psi_\alpha\rangle_A A_k|\alpha\rangle_B|k\rangle_E \tag{51}$$

Subsequently, we consider projected version of the state

$$|\tilde{\psi}_{ABE}\rangle = I_A\otimes\Pi_E\otimes\Pi_B|\psi_{ABE}\rangle. \tag{52}$$

This state can be written as

$$|\tilde{\psi}_{ABE}\rangle = \frac{1}{\sqrt{N}} \sum_{\alpha,k} |\psi_\alpha\rangle_A F_k |\alpha\rangle_B |k\rangle_E \tag{53}$$

where recall that $F_k = \Pi_B A_k$, and we sum only over typical indices k.

Let us now prove that with high probability, the state $\tilde{\psi}_{ABE}$ will be close to the actual state ψ_{ABE} shared by Alice, Bob and Eve.

Proposition 4 (Typicality does not hurt I) *For arbitrary* $0 < \epsilon < 1$, *for* n *large enough we have*

$$|| \, |\psi_{ABE}\rangle\langle\psi_{ABE}| - |\tilde{\psi}_{ABE}\rangle\langle\tilde{\psi}_{ABE}| \, || \leq \epsilon \tag{54}$$

with high probability for any normalized codes satisfying $\int |\alpha\rangle\langle\alpha| \mathrm{d}a\, lpha = \rho_A^{typ}$

Proof. From lemma 9 it follows that it is enough to prove that for n large enough we have

$$|\langle\tilde{\psi}_{ABE}|\psi_{ABE}\rangle|^2 \geq 1 - \epsilon \tag{55}$$

We will show now that it is true with high probability. We have

$$|\langle\psi|I_E \otimes \Pi_B \otimes \Pi_E|\psi\rangle|^2 = \frac{1}{N} \sum_\alpha \mathrm{Tr}(\sum_k F_k^\dagger F_k |\alpha\rangle\langle\alpha|) \tag{56}$$

We note that

$$\left\langle |\langle\psi|I_E \otimes \Pi_B \otimes \Pi_E|\psi\rangle|^2 \right\rangle_\alpha = \mathrm{Tr} \sum_k F_k \rho_A^{typ} F_k^\dagger = \mathrm{Tr}\rho'_B \tag{57}$$

From proposition 3, Eq. (35) it follows that for n large enough we have $\mathrm{Tr}\rho'_B \geq 1 - \epsilon^2$. The random variable $1 - |\langle\psi|I_E \otimes \Pi_B \otimes \Pi_E|\psi\rangle|^2$ is nonnegative, so we can use Markov inequality obtaining

$$Prob(|\langle\psi|I_E \otimes \Pi_B \otimes \Pi_E|\psi\rangle|^2 \leq 1 - 2\epsilon) \leq \epsilon \tag{58}$$

This ends the proof. ∎

Remark. Note that in proof we have only used the fact that codewords are normalized, and picked from an ensmeble whose density matrix is ρ_A^{typ}.

B. Unnormalized codes

If codewords are not normalized, Alice prepares the following state:

$$\psi_{AA'} = \frac{1}{\sqrt{\sum_{\alpha=1}^N \langle\alpha|\alpha\rangle}} \sum_{\alpha=1}^N |\psi_\alpha\rangle_A \otimes |\alpha\rangle_{A'} \tag{59}$$

The emerging Alice, Bob and Eve state is then

$$\psi_{ABE} = \frac{1}{\sqrt{\sum_{\alpha=1}^N \langle\alpha|\alpha\rangle}} \sum_\alpha \sum_{k\in K} |\psi_\alpha\rangle_A A_k |\alpha\rangle_B |k\rangle_E \tag{60}$$

We will consider unnormalized version of this state

$$\psi'_{ABE} = \psi_{ABE}(\mathcal{C}) = \frac{1}{\sqrt{N}} \sum_\alpha \sum_{k\in K} |\psi_\alpha\rangle_A A_k |\alpha\rangle_B |k\rangle_E \tag{61}$$

and project it onto typical subspaces, obtaining

$$|\tilde{\psi}_{ABE}\rangle = \frac{1}{\sqrt{N}} \sum_{\alpha,k} |\psi_\alpha\rangle_A F_k |\alpha\rangle_B |k\rangle_E. \tag{62}$$

We will now show that for uniform ρ_A^{typ}-deformed codes the state $\tilde{\psi}_{ABE}$ is close in trace norm to the actual state ψ_{ABE} shared by Alice and Bob.

Proposition 5 (Typicality does not hurt II) *For arbitrary $0 < \epsilon < 1$, for n large enough we have*

$$|| \, |\psi_{ABE}\rangle\langle\psi_{ABE}| - |\tilde{\psi}_{ABE}\rangle\langle\tilde{\psi}_{ABE}| \, || \leq \epsilon \tag{63}$$

with high probability for uniform ρ_A^{typ} -deformed codes.

Proof. From lemma 9 it follows that we have to show that with high probability we have

$$|\langle\psi'_{ABE}|\tilde{\psi}_{ABE}\rangle|^2 \geq 1 - \epsilon \tag{64}$$

and

$$\langle\psi'_{ABE}|\psi'_{ABE}\rangle \leq 1 + \epsilon. \tag{65}$$

The last inequality reads as

$$\frac{1}{N}\sum_\alpha \langle\alpha|\alpha\rangle \leq 1 + \epsilon \tag{66}$$

We will now compute average and variance of this quantity over codes. Using (47) we get

$$\Big\langle \frac{1}{N}\sum_\alpha \langle\alpha|\alpha\rangle \Big\rangle_{\mathcal{C}} = \Big\langle \langle\alpha|\alpha\rangle \Big\rangle_{\mathcal{C}} = 1 \tag{67}$$

and

$$Var = Var(\langle\alpha|\alpha\rangle) \leq (1+\epsilon) 2^{-n(S_A - \delta)} \tag{68}$$

since codewords are picked independently. Thus form Chebyshev inequality we get

$$Prob(|\frac{1}{N}\sum_i X_i - 1| \geq \epsilon) \leq \frac{1+\epsilon}{\epsilon^2} \, 2^{-n(S_A-\delta)} \tag{69}$$

Thus with high probability the inequality (65) is satisfied. To prove the same for inequality (64) we write

$$|\langle\psi'|I_E \otimes \Pi_B \otimes \Pi_E|\psi'\rangle|^2 = \frac{1}{N}\sum_\alpha \mathrm{Tr}(\sum_k F_k^\dagger F_k |\alpha\rangle\langle\alpha|) \equiv \frac{1}{N}\sum_{i=1}^N X_i \tag{70}$$

where X_i defined by the above equality are i.i.d random variables. We note that

$$\big\langle X_i \big\rangle_\alpha = \mathrm{Tr}\sum_k F_k \rho_A^{typ} \, F_k^\dagger = \mathrm{Tr}\rho'_B \geq 1 - \epsilon \tag{71}$$

We compute variance.

$$Var(\frac{1}{N}\sum_i X_i) = Var X_i = \Big\langle \langle\alpha|Y|\alpha\rangle\langle\alpha Y|\alpha\rangle \Big\rangle_\alpha - (\mathrm{Tr}\rho'_B)^2 \tag{72}$$

where $Y = \sum_k F_k^\dagger F_k$. For particular case of uniform ρ_A^{typ} -deformed codes we obtain

$$Var \leq \mathrm{Tr} Y \rho_A^{typ} \, Y \rho_A^{typ} \, + (\mathrm{Tr} Y \rho_A^{typ} \,)^2 - (\mathrm{Tr}\rho'_B)^2 = \mathrm{Tr}\rho_B'^2 \leq (1+\epsilon) 2^{-n(S_B - \delta)} \tag{73}$$

where we have used $\mathrm{Tr}(\sum_k F_k^\dagger F_k \rho_A^{typ} \,) = \mathrm{Tr}\rho'_B$. Using Chebyshev inequality we get

$$Prob(|\langle\tilde{\psi}_{ABE}|\psi_{ABE}\rangle|^2 \leq 1 - \epsilon) \leq \frac{1-\epsilon}{\epsilon^2} \, 2^{-n(S_B - \delta)} \tag{74}$$

This proves that with high probability, also the inequality (64) is satisfied. This ends the proof. ∎

VIII. CODING THEOREM VIA DISTINGUISHABILITY AND PRIVACY.

In this section we prove the main result of this paper: direct coding theorem by use of distinguishability and privacy. Our proof will show that for normalized random codes, only two conditions assure that the codes can bse used in coding theorem:

1) The ensemble gives rise to ρ_A^{typ}.

2) Privacy: codewords produce indistinguishable Eve's output states.

We see that these are quite modest conditions.

A. Bob's and Eve's output states.

It is useful to write down Alice and Bob's output states in terms of Kraus operators. We have

$$\sigma_\alpha^E = \sum_{k,k'\in K} \mathrm{Tr}(A_k|\alpha\rangle\langle\alpha|A_{k'}^\dagger)|k\rangle\langle k'| \tag{75}$$

$$\sigma_\alpha^B = \sum_{k\in K}(A_k|\alpha\rangle\langle\alpha|A_k^\dagger) \equiv \Lambda^{\otimes n}(|\alpha\rangle\langle\alpha|) \tag{76}$$

$$\tag{77}$$

Now, we introduce modified states ${\sigma_E^\alpha}'$ and ${\sigma_B^\alpha}'$ given by

$${\sigma_E^\alpha}' = \sum_{k,k'} \mathrm{Tr}(F_k|\alpha\rangle\langle\alpha|F_{k'}^\dagger)|k\rangle\langle k'| \tag{78}$$

$${\sigma_B^\alpha}' = \sum_k F_k|\alpha\rangle\langle\alpha|F_k^\dagger \tag{79}$$

These states are reductions of the state 53, 62. For normalized codes, the states are subnormalized, while for unnormalized codes, their trace may be both below and above 1. They have the following properties. For any code satisfying $\int|\alpha\rangle\langle\alpha|\mathrm{d}\alpha = \rho_A^{typ}$ we obtain

$$\int {\sigma_E^\alpha}'\mathrm{d}\alpha = \rho_E', \quad \int {\sigma_B^\alpha}'\mathrm{d}\alpha = \rho_B' \tag{80}$$

Moreover due to propositions 4 and 5, and monotonicity of trace norm under trace preserving CP maps, they are close on average to the original states σ_α^E, σ_α^B, which is stated in the following lemma

Lemma 4 *For arbitrary $0<\epsilon<1/2$ and for n high enough, with high probability we have*

$$\frac{1}{N}\sum_\alpha ||\sigma_\alpha^E - {\sigma_E^\alpha}'|| \leq \epsilon, \quad \frac{1}{N}\sum_\alpha ||\sigma_\alpha^B - {\sigma_B^\alpha}'|| \leq \epsilon. \tag{81}$$

where ϵ is independent on N, and can be taken to be exponential in n.

Recall, that ϵ is exponential in n.

B. Privacy

We first prove that if $N = 2^{nR}$ with $R < I_{coh}$ then the distinguishability by Eve is arbitrarily small. Let us first bound χ_E by average norm distance. We apply Fannes inequality [15]

$$|S(\rho) - S(\sigma)| \leq ||\sigma-\rho||\log d + \eta(||\sigma-\rho||) \tag{82}$$

where ρ and σ are any states satisfying $||\rho-\sigma|| < 1/3$, $\eta(x) = -x\log x$, and d is dimension of the Hilbert space. Denoting $\frac{1}{N}\sum_{\alpha\in\mathcal{C}}||\sigma_E^\alpha - \sigma_E|| = x$, and using convexity of η we obtain

$$\chi_E = \chi_E \leq xn\log d + \eta(x) \tag{83}$$

where d is input dimension of Hilbert space of ρ_A (i.e. it is a constant). Thus if we show that $\frac{1}{N}\sum_{\alpha\in\mathcal{C}}||\sigma_E^\alpha - \sigma_E||$ is exponentially small for rate $R < I_{coh}$, then also χ_E will be exponentially small.

Proposition 6 *(privacy). For the state ψ_{ABE} and $N = 2^{nR}$ where $R < I_{coh}$ with high probability (over codes) we have*

$$\frac{1}{N}\sum_{\alpha\in\mathcal{C}} ||\sigma_E^\alpha - \sigma_E|| \leq \epsilon. \tag{84}$$

Proof. First we note that

$$||\sigma_E^\alpha - \sigma_E|| \leq ||\sigma_E^\alpha - \rho'_E|| + ||\sigma_E - \rho'_E|| \leq 2||\sigma_E^\alpha - \rho'_E|| \tag{85}$$

In the last inequality we have used convexity of norm, and the fact that σ_E is mixture of σ_E^α. Subsequently we have

$$||\sigma_E^\alpha - \rho'_E|| \leq ||\sigma_E^\alpha - \sigma_E^\alpha{}'|| + ||\sigma_E^\alpha{}' - \rho'_E|| \tag{86}$$

Using (81) we finally get

$$\frac{1}{N}\sum_\alpha ||\sigma_E^\alpha - \sigma_E|| \leq 2\epsilon + \frac{1}{N}\sum_\alpha ||\sigma_E^\alpha{}' - \rho'_E|| \tag{87}$$

Thus we have to estimate $||\sigma_E^\alpha{}' - \rho'_E||$. To this end we use lemma 8 and get

$$||\sigma_E^\alpha{}' - \rho'_E||^2 \leq d\mathrm{Tr}(\sigma_E^\alpha{}' - \rho'_E)^2 \tag{88}$$

where d is dimension of the Hilbert space on which both ρ'_E and $\sigma_E^\alpha{}'$ act. We note that

$$\sigma_E^\alpha{}' = \Gamma(|\alpha\rangle\langle\alpha|), \quad \rho'_E = \Gamma(\rho_A^{typ}) \tag{89}$$

where Γ is a CP map. Then due to lemma 7 we have
Thus we have

$$\mathrm{supp}\,(\sigma_\alpha) \subset \mathrm{supp}\,(\rho'_E) \tag{90}$$

so that the dimension d can be chosen as dimension of support of ρ'_E. Thus due to Eq. (37) which says that rank of ρ'_E is bounded by rank of $\hat\rho_E^{typ}$ we have

$$d \leq 2^{n(S_E+\delta)} \tag{91}$$

Now, we compute average square of Hilbert-Schmidt distance for Seth's codes

$$\left\langle \mathrm{Tr}(\sigma_E^\alpha{}' - \rho'_E)^2\right\rangle_\alpha = \left\langle \mathrm{Tr}(\sigma_E^\alpha{}')^2\right\rangle_\alpha + \mathrm{Tr}\rho_E'^2 - 2\left\langle \mathrm{Tr}(\sigma_E^\alpha{}'\rho'_E)\right\rangle_\alpha \tag{92}$$

We have

$$\left\langle \mathrm{Tr}(\sigma_E^\alpha{}')^2\right\rangle_\alpha = \sum_{kk'}\int \langle\alpha|F_{k'}^\dagger F_k|\alpha\rangle\langle\alpha|F_k^\dagger F_{k'}|\alpha\rangle = \mathrm{Tr}\rho_E'^2 + \mathrm{Tr}\rho_B'^2 - \mathrm{Tr}\rho_{i/o}^2 \leq \mathrm{Tr}\rho_E'^2 + \mathrm{Tr}\rho_B'^2 \tag{93}$$

and

$$\left\langle \mathrm{Tr}\sigma_E^\alpha{}'\rho'_E\right\rangle_\alpha = \mathrm{Tr}\rho_E'^2 \tag{94}$$

So that

$$\left\langle \mathrm{Tr}(\sigma_E^\alpha{}' - \rho'_E)^2\right\rangle_\alpha \leq \mathrm{Tr}\rho_B'^2 \leq 2^{-n(S_B-\delta)} \tag{95}$$

The same we obtain for uniform ρ_A^{typ}-deformed codes. Then from eqs. (91), (95) and (88) we get

$$\left\langle ||\sigma_E^\alpha{}' - \rho'_E||^2\right\rangle_\alpha \leq 2^{-n(I_{coh}+\delta)} \tag{96}$$

Hence also

$$\left\langle \frac{1}{N}\sum_\alpha ||\sigma_E^\alpha{}' - \rho'_E||^2\right\rangle_\alpha \leq 2^{-n(I_{coh}+\delta)} \tag{97}$$

By Markov inequality we then obtain

$$Prob(||\rho_E^\alpha - \rho'_E||^2 \geq \epsilon) \leq \frac{1}{\epsilon^2} 2^{-n(I_{coh}+\delta)} \tag{98}$$

Due to equation (87) we get

$$\frac{1}{N}\sum_\alpha ||\sigma_E^\alpha - \sigma_E|| \leq 3\epsilon \tag{99}$$

with high probability over codes. This ends the proof of the proposition. Recall, that ϵ can be taken exponential in n. ∎

C. Distinguishability

Here we prove that Bob's outputs are distinguishable for $R < I_{coh}$.

To show that χ_B is close to $\log N$ it is enough that for a random code with $R < I_{coh}$ is distinguishable by some measurement, with probability of error exponentially small. This can be shown again by referring to Fannes inequality. Let outcomes of POVM be denoted by β. Then by Fannes inequality we obtain that the mutual information between input signals α, and the measurement output satisfies

$$I(\alpha:\beta) \geq \log N - (8p_e n \log d + 3\eta(p_e)) \tag{100}$$

where p_e is probability of error

$$p_e = 1 - \frac{1}{N}\sum_{\alpha=\beta} p(\beta|\alpha) \tag{101}$$

with $p(\beta|\alpha)$ is probability of obtaining outcome β given the state was ${\sigma_B^\alpha}'$. Since postprocessing can only decrease mutual information, we have

$$\chi_B' \geq I(\alpha:\beta). \tag{102}$$

Thus, if we can show that for a random code, Bob's output states are distinguishable by some measurement with exponentially small (in n) probability of error.

To this end we will modify a result due to Devetak [8]:

Lemma 5 *Assume that an ensemble $\{p_i, \rho_i : i \in S\}$ with $\sum_i p_i\rho_i = \rho$ such that there exist projectors Π_i, Π satisfying*

$$\mathrm{Tr}\rho_i P \geq 1-\epsilon \tag{103}$$
$$\mathrm{Tr}\rho_i \Pi_i \geq 1-\epsilon \tag{104}$$
$$\mathrm{Tr}\Pi_i \leq 2^{nL} \tag{105}$$
$$\Pi\rho\Pi \leq 2^{-nG}\Pi \tag{106}$$

Then there exists a subset $\mathcal{C}$ of S of size $2^{n[G-L-\delta]}$ and a corresponding POVM $\{Y_i\}$ which reliably distinguishes between the ρ_i from $\mathcal{C}$ in the sense that

$$p_s = \frac{1}{|\mathcal{C}|}\sum_{i\in\mathcal{C}} \mathrm{Tr}\rho_i Y_i \geq 1 - 2(\epsilon + \sqrt{8\epsilon}) - 4\times 2^{-n\delta} \tag{107}$$

In our case the role of ρ_i will be played by output Bob states σ_B^α. However we cannot use the lemma directly, as in some case we do not have information about those state for each particular α. Rather, we have information about some average.

Our goal is to evaluate probability of success p_s for distinguishing randomly chosen N states σ_α^B. Instead, we will first evaluate average of the following quantity

$$\tilde{p}_s = \frac{1}{N}\sum_\alpha \mathrm{Tr}{\sigma_B^\alpha}' Y_\alpha \tag{108}$$

where Y_α is some suitably chosen POVM. Since ${\sigma_B^\alpha}'$ are not normalized, this does not have interpretation of probability of success. However we will now show, that p_s is close to $\tilde{p}_s$.

Lemma 6 *Let $\epsilon > 0$. Then for n large enough,*

$$p_s = \frac{1}{N}\sum_\alpha \mathrm{Tr}(\sigma_B^\alpha Y_\alpha) \geq \frac{1}{N}\sum_\alpha \mathrm{Tr}({\sigma_B^\alpha}' Y_\alpha) - \epsilon \tag{109}$$

Proof. Using inequality $|\mathrm{Tr}(AB)| \leq ||A|| ||B||_{op}$ where $||\cdot||_{op}$ is operator norm, we obtain

$$\mathrm{Tr}[(\sigma_B^\alpha - {\sigma_B^\alpha}')Y_\alpha] \leq ||\sigma_B^\alpha - {\sigma_B^\alpha}'|| \times ||Y_\alpha||_{op} \tag{110}$$

Since Y_α are elemnts of POVM, we have $||Y_\alpha||_{op} \leq 1$. Thus we get

$$\frac{1}{N}\sum_\alpha \mathrm{Tr}(\sigma_B^\alpha Y_\alpha) \geq \frac{1}{N}\sum_\alpha \mathrm{Tr}({\sigma_B^\alpha}' Y_\alpha) - \frac{1}{N}\sum_\alpha ||\sigma_B^\alpha - {\sigma_B^\alpha}'||. \tag{111}$$

From lemma 4 we know that the last term is arbitrary small for n large enough, hence we obtain the required estimate. ▮

Thus it is enough to estimate the quantity $\tilde{p}_s$. Below we will show that on average the quantity $\tilde{p}_e = 1 - \tilde{p}_s$ is exponentially small, provided $N = 2^{nR}$, with $R < I_{coh}$.

Proposition 7 *Fix arbitrary $\epsilon > 0$ and n large enough. Consider code $\mathcal{C}$ consisting of $N = 2^{nR}$ codewords $|\alpha\rangle$ where $R < I_{coh}$. Then there exists POVM $\{Y_\alpha\}$ such that*

$$\Big\langle \frac{1}{N} \sum_\alpha \mathrm{Tr}(\sigma_B^\alpha{}' Y_\alpha) \Big\rangle_{\mathcal{C}} \leq \epsilon. \tag{112}$$

Proof. Let us recall important for us properties of states $\sigma_B^\alpha{}'$. We have

$$\mathrm{rk}\, \sigma_B^\alpha{}' = \mathrm{rk}\, \sigma_E^\alpha{}' = d_E \leq 2^{-n(S_E - \delta)}, \tag{113}$$

$$\Pi_B \sigma_B^\alpha{}' \Pi_B = \sigma_B^\alpha{}', \tag{114}$$

$$\int \sigma_B^\alpha{}' \mathrm{d}\alpha = \rho_B' \tag{115}$$

For a fixed N element code $\mathcal{C}$, we have the correspoding set of states $\sigma_B^\alpha{}'$, we choose POVM as

$$Y_\alpha = (\sum_{\alpha' \in \mathcal{C}} \Lambda_{\alpha'})^{-1/2} \Lambda\alpha (\sum_{\alpha' \in \mathcal{C}} \Lambda_{\alpha'})^{-1/2} \tag{116}$$

with

$$\Lambda_\alpha = \Pi_B^\alpha \Pi_B \Pi_B^\alpha \tag{117}$$

where Π_B^α is a projector onto support of $\sigma_B^\alpha{}'$. We then know that $\mathrm{Tr}\Pi_B^\alpha \leq 2^{-n(S_E-\delta)}$. We will use operator inequality proven by Nagaoka and Hayashi [16]

$$I - (S+T)^{-1/2} S (S+T)^{-1/2} \leq 2(1-S) + 4T \tag{118}$$

valid for any operators satisfying $0 \leq S \leq I$ and $T \geq 0$. Using it we can evaluate average of $\tilde{p}_e$ over codes as follows

$$\langle \tilde{p}_e \rangle_{\mathcal{C}} = 1 - \Big\langle \frac{1}{N} \sum_\alpha \mathrm{Tr} \sigma_B^\alpha{}' Y_\alpha \Big\rangle_\alpha \leq 2(1 - \langle \mathrm{Tr}(\sigma_B^\alpha{}' \Lambda_\alpha) \rangle_\alpha + 4 \sum_{\alpha' \neq \alpha} \langle \mathrm{Tr}(\sigma_B^\alpha{}' \Lambda_{\alpha'}) \rangle_{\alpha,\alpha'} \tag{119}$$

Using (114) we get $\mathrm{Tr}(\sigma_B^\alpha{}'\Lambda_\alpha) = \mathrm{Tr}\sigma_B^\alpha{}'$ so that $\langle \mathrm{Tr}(\sigma_B^\alpha{}' \Lambda_\alpha \rangle_\alpha = \mathrm{Tr}\rho_B'$. Since $\alpha's$ are drawn independently,

$$\sum_{\alpha' \neq \alpha} \langle \mathrm{Tr}\sigma_B^\alpha{}' \Lambda_{\alpha'} \rangle_{\alpha,\alpha'} = (N-1)\mathrm{Tr}(\rho_B' \langle \Pi_B^\alpha \rangle) \leq (N-1) ||\rho_B'||_{op} \langle \mathrm{Tr}\Pi_B^\alpha \rangle_\alpha \leq (N-1) 2^{n(S_E+\delta)} (1+\epsilon) 2^{-n(S_B-\delta)} \tag{120}$$

where we have used properties of state ρ_B' form section V A. we see that if $R < S_B - S_E$ then $\tilde{p}_e$ goes down exponentially. This ends the proof of proposition ▮

In this way we have proven second ingredient of the quantum coding theorem. It is instructive to see what properties of code we have used in this section. We have based solely on the fact that the code ensemble gives rise to density matrix ρ_A^{typ}, and that the actual state ψ_{ABE} is close to projected state ψ_{ABE}. We have shown in section VII for normalized codes, the latter property follows from the former one. Thus for normalized codes, distignuishability by Bob is guaranteed by the fact that we draw codes from ensemble of typical version of course density matrix. For unnormalized codes, the condition "actual close to projected" needs to be checked, but once it is satisfied for a given code, we obtain distinguishability again for free.

IX. CONCLUSIONS

In this paper we have considered quantum coding theorem with random quantum codes. We have managed to divide the problem into two subproblems: checking that codewords are distinguishable by receiver (Bob) and indistinguishable by the one who controls environment (Eve). For normalized codes, we have shown that distinguishability by Bob is matched, when we draw code form whatever ensemble of typical version of source density matrix. In contrast, we have not exhibited general conditions, which ensure privacy (indistiguishability by Eve). We have checked them for two types of codes which we have considered. We hope that this paper will also provide insight into problem of coding in more general type of channels.

Acknowledgements

MH is supported by Polish Ministry of Scientific Research and Information Technology under the (solicited) grant no. PBZ-MIN-008/P03/2003 and EC IP SCALA.

X. APPENDIX

A. Supports

Lemma 7 *For any states* σ, ρ *if* $\mathrm{supp}\,(\sigma) \subset \mathrm{supp}\,(\rho)$ *then for any CP map also* $\mathrm{supp}\,(\Lambda(\sigma)) \subset \mathrm{supp}\,(\Lambda(\rho))$.

Proof. We leave this ass an exercise for the reader.

B. Norms and fidelity

The following lemma that relates trace norm with Hilbert Schmidt norm

Lemma 8 *For any hermitian operator* X *we have*

$$||X||_{\mathrm{Tr}}^2 \leq d||X||_{HS}^2 \tag{121}$$

where d *is dimension of the support of operator* X *(the subspace on which* X *has nonzero eigenvalues), and* $||\cdot||_{HS}$ *is Hilbert-Schmidt norm, given by*

$$||X|| = \sqrt{\mathrm{Tr}X^2} \tag{122}$$

for any Hermitian operator X.

Proof. It it implied by convexity of function x^2, where one takes probabilities $1/d$. ∎

The fidelity given by

$$F(\rho,\sigma) = \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{r}ho} \tag{123}$$

is related to trace norm as follows [10]

$$1 - F \leq \frac{1}{2}||\rho - \sigma|| \leq \sqrt{(}1 - F(\rho,\sigma))^2 \tag{124}$$

We will also need the following lemma

Lemma 9 *For any vector* ψ' *and* $\tilde{\psi} = \Pi\psi'$ *where* Π *is a projector, where* $|\langle\tilde{\psi}|\psi'\rangle|^2 \geq 1-\epsilon$, $\langle\psi'|\psi'\rangle \leq 1+\epsilon$ *and* $0 < \epsilon < 1$ *we have*

$$||\,|\tilde{\psi}\rangle\langle\tilde{\psi}| - |\psi\rangle\langle\psi|\,|| \leq 6\sqrt{\epsilon} \tag{125}$$

where ψ *denotes normalized version of* ψ', *i.e.* $\psi = \psi'/\sqrt{\langle\psi'|\psi'\rangle}$

Proof. For any vector $|v\rangle$ denote $P_v = |v\rangle\langle v|$. We then have

$$||P_{\tilde{\psi}} - P_\psi|| \leq ||P_{\tilde{\psi}} - \frac{P_{\tilde{\psi}}}{\mathrm{Tr}P_{\tilde{\psi}}}|| + ||\frac{P_{\tilde{\psi}}}{\mathrm{Tr}P_{\tilde{\psi}}} - P_\psi|| \leq |1 - \langle\tilde{\psi}|\tilde{\psi}\rangle| + 2\sqrt{1 - \frac{|\langle\tilde{\psi}|\psi\rangle|^2}{\langle\tilde{\psi}|\tilde{\psi}\rangle}} \tag{126}$$

where we have used inequality (124). Subsequently, we get

$$||P_{\tilde{\psi}} - P_\psi|| \leq |1 - \langle\tilde{\psi}|\tilde{\psi}\rangle| + 2\sqrt{1 - \frac{|\langle\tilde{\psi}|\psi'\rangle|^2}{\langle\psi'|\psi'\rangle}} \tag{127}$$

Now, form assumptions of the lemma, it follows that $(1-\epsilon)/(1+\epsilon) \leq \langle\tilde{\psi}|\tilde{\psi}\rangle \leq 1+\epsilon$. This together with the assumptions gives

$$||P_{\tilde{\psi}} - P_\psi|| \leq 2\epsilon + 2\sqrt{1 - \frac{1-\epsilon}{(1+\epsilon)^2}} \leq 6\sqrt{\epsilon} \tag{128}$$

This ends the proof of the lemma. ∎

C. Averaging over codewords

In this section we will present useful formulas for averaging over codewords.

From [1] we get the following rules for Lloyd codes.

$$\int \langle\alpha|X|\alpha\rangle\langle\alpha|Y|\alpha\rangle \mathrm{d}\alpha = \sum_{ij} p_i p_j \langle i|X|i\rangle\langle j|Y|j\rangle + \sum_{ij} p_i p_j \langle i|X|j\rangle\langle j|Y|i\rangle - \sum_i p_i^2 \langle i|X|i\rangle\langle i|Y|i\rangle =$$
$$= \mathrm{Tr}(X\rho_A^{typ})\mathrm{Tr}(Y\rho_A^{typ}) + \mathrm{Tr}(X\tilde{\rho}_A Y\rho_A^{typ}) - \sum_i p_i^2 \langle i|X|i\rangle\langle i|Y|i\rangle \tag{129}$$

for any operators X, Y. For uniform ρ_A^{typ}-deformed codes, we use properties of projector onto symmetric subspace and get

$$\int \langle\alpha|X|\alpha\rangle\langle\alpha|Y|\alpha\rangle \mathrm{d}\alpha = \frac{d_A}{d_A+1}\left[\mathrm{Tr}(X\rho_A^{typ})\mathrm{Tr}(Y\rho_A^{typ}) + \mathrm{Tr}(X\tilde{\rho}_A Y\rho_A^{typ})\right] \tag{130}$$

for any operators X, Y. For both codes we have

$$\int |\alpha\rangle\langle\alpha| \mathrm{d}\alpha = \rho_A^{typ} \tag{131}$$

[1] S. Lloyd, Phys. Rev. A **55**, 1613 (1997), quant-ph/9604015.
[2] H. Barnum, M. A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).
[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett **85**, 433 (2000), quant-ph/0003040.
[4] P. W. Shor (2002), talk at MSRI Workshop on Quantum Computation. Available online under `http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/`.
[5] I. Devetak, quant-ph/0304127.
[6] I. Devetak and A. Winter, Proc. R. Soc. Lond. A (2005), quant-ph/0306078.
[7] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996), quant-ph/9604022.
[8] I. Devetak, unpublished.
[9] B. Schumacher and M. D. Westmoreland, quant-ph/0112106.
[10] C. A. Fuchs and J. van de Graaf (1997), quant-ph/9712042.
[11] M. Ohya and D. Petz, *Quantum entropy and its use* (Springer-Verlag, Heidelberg, 1993).
[12] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
[13] J. A. Smolin, F. Verstraete, and A. Winter, Phys. Rev. A **72**, 052317 (2005), quant-ph/0505038.
[14] T. M. Cover and J. A. Thomas, *Elements of information theory* (Wiley, 1991).
[15] M. Fannes, Commun. Math. Phys. **31**, 291 (1973).
[16] M. Hayashi and H. Nagaoka, quant-ph/0206186.